

What is claimed is:

Sub B1
1. A system for managing handwritten signatures, comprising:

(a) a graphic tablet for signaling position coordinates of a stylus during manual movement thereof relative to a writing surface;

(b) a clock circuit for periodically initiating position measurements by the graphic tablet at predetermined fixed time intervals;

(c) a first computer processor electrically interfaced with the tablet, the processor being programmed for receiving a multiplicity of the coordinates during the manual movement of the stylus, and storing respective sets of the coordinates in sequential order as an electronic signature while preserving a time relation between coordinates, the electronic signature forming a time history of the stylus movement; and

(d) means for verifying the fixed time intervals of the measurements.

2. The system of claim 1, further comprising means for comparing the electronic signature with a reference signature.

Sub A1
3. The system of claim 2, wherein the means for comparing comprises reference memory for storing an electronic counterpart of the reference signature, and a cross-correlator for evaluating a degree of correspondence between respective time histories of the electronic signature and the electronic counterpart of the reference signature.

24

001634 421600

³
~~4.~~ The system of claim ²~~3~~, wherein the reference memory is electronically interfaced with the first computer processor.

5. The system of claim 2, wherein the means for comparing comprises the computer processor having a graphic display implemented for simultaneously displaying the electronic signature and the reference signature with corresponding cursors being positioned along a line segment of the signature and oriented perpendicular to the line segment, and the computer being further implemented for moving the cursors in response to operator input.

⁴
~~6.~~ The system of claim 1, wherein the electronic signature has associated therewith a date and time of the handwritten signature.

⁵
~~7.~~ The system of claim ⁴~~6~~, wherein the electronic signature has further associated therewith an annotation including at least one of a geographic location, a physical address, and an identification string.

⁶
~~8.~~ The system of claim 1, wherein the first computer processor is a digital processor, and the electronic signature is a digital signature.

⁹
~~9.~~ The system of claim 1, wherein the graphic tablet includes the clock circuit.

¹²
~~10.~~ The system of claim ¹¹~~9~~, wherein the time intervals are not greater than 20 milliseconds.

¹³
~~11.~~ The system of claim ¹²~~10~~, wherein the time intervals are between 2 milliseconds and 3 milliseconds.

25

00215415-12580

12. The system of claim 9, wherein the means for verifying the time intervals comprises the computer being programmed for determining a ratio of a total elapsed time of the measurements and a total number of the measurements, and comparing the ratio with the predetermined interval.

pub
102 13. The system of claim 9, wherein the means for verifying the time intervals comprises

(a) the clock circuit having a certified unalterable time interval;

(b) the tablet being implemented for transmitting an encoded certification stamp with the coordinate data; and

(c) the computer being programmed for for decoding the certification stamp to verify use of the certified time interval.

7
14. The system of claim 1, wherein the computer is further programmed for encrypting the time history to a fixed key of arbitrary length, the stored electronic signature being in encrypted form.

8
7
15. The system of claim 14, wherein the computer is programmed for generating the key as a cryptographic hash function or message digest of the document.

pub
103 16. A method for electronically signing a document, comprising the steps of:

(a) progressively capturing a handwritten signature as an ordered sequence of data corresponding to successive coordinates and corresponding timing of stylus movement producing the signature;

26

(a) embedding the signature receipt into the document; and

(b) embedding the document receipt into the electronic signature, thereby to form a cross-linked binding of the signature with the document.

27. The method of claim 25, wherein the step of producing the receipt counterparts comprises the further steps of:

- (a) providing a transportable file medium;
- (b) copying counterparts of the document receipt and the signature receipt on the file medium; and
- (c) delivering the file medium having the receipt counterparts to a signer of the document.

18
28. A method for verifying the signature of an electronically signed a document having associated therewith an electronic signature being a stored sequence of data corresponding to coordinates of stylus movement producing a first handwritten signature:

(a) capturing a second electronic signature as a stored sequence of data corresponding to coordinates of stylus movement producing second handwritten signature;

(b) simultaneously displaying in locational proximity graphic counterparts of the first and second electronic signatures;

(c) displaying, for each of the graphic counterparts, a cursor being positioned along a line segment of the signature and oriented perpendicular to the line segment; and

(d) for each of the graphic counterparts, moving the cursor relative to the signature in response to operator input.

27

(a) determining at least one measurement parameter relative to the line segment at which the cursor is located; and

²⁰
~~30.~~ The method of claim ¹⁹~~29~~, wherein the at least one measurement parameter is selected from the group consisting of a point number, a stroke number, an acceleration value, and a pressure value.

add 7

Add Pg

28

[illegible]

(c) electronically binding the electronic signature to a stored counterpart of the document.

(a) creating an encryption key by generating a cryptographic hash function or message digest of the stored counterpart of the document, and

18. The method system of claim 17, comprising the further steps of identifying stored instances of the encryption key and erasing each such instance.

(a) capturing a handwritten signature as a sequence of data corresponding to coordinates of stylus movement producing the signature;

(c) creating an encryption key by generating a cryptographic hash function or message digest of a stored counterpart of the document;

(e) identifying stored instances of the encryption key; and

(f) erasing each stored instance of the encryption key.

20. The method of claim 19, wherein the step of storing comprises the further steps of:

- (a) encrypting the sequence of data to a fixed key of arbitrary length; and
- (b) storing the encrypted sequence as the electronic signature.

21. The method of claim 19, wherein the step of storing comprises the further steps of:

- (a) determining a date and time at which the handwritten signature was produced;
- (b) including counterparts of the date and time with the electronic signature.

22. The method of claim 21, wherein the step of storing comprises the further steps of:

- (a) determining a set of document data associated with the document;
- (b) generating a cryptographic hash data string of arbitrary length from the document data; and
- (c) encrypting the electronic signature using the cryptographic hash data string.

23. The method of claim 19, comprising the further step of electronically tying the encrypted signature to the stored counterpart of the document using a device selected from the set consisting of forming a linked directory structure, forming a database, forming a compressed file, and forming a common digital signature packet.

2025 RELEASE UNDER E.O. 14176

24. A method for decrypting a signature having been encrypted by the method of claim 19 to facilitate authentication of the binding, comprising the further steps of:

- (a) creating a counterpart of the encryption key by generating another cryptographic hash function or message digest of the stored counterpart of the document;
- (b) decrypting the electronic signature using the encryption key, thereby electronically binding the electronic signature to a stored counterpart of the document;
- (c) identifying stored instances of the encryption key; and
- (d) erasing each stored instance of the encryption key.

25. A method for electronically signing a document, comprising the steps of:

- (a) capturing a handwritten signature as a sequence of data corresponding to coordinates of stylus movement producing the signature;
- (b) storing the data as an electronic signature;
- (c) creating a signature receipt as a cryptographic hash function or message digest of the electronic signature;
- (d) creating a document receipt as a cryptographic hash function or message digest of a stored counterpart of the document; and
- (e) producing counterparts of the signature and document receipts.

26. The method of claim 25, comprising the further steps of:

2025 RELEASE UNDER E.O. 14176